



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,960	12/12/2003	David Carroll Challener	RPS920030198US1	1316

45211 7590 04/19/2006

KELLY K. KORDZIK  
WINSTEAD SECHREST & MINICK PC  
PO BOX 50784  
DALLAS, TX 75201

EXAMINER

RAHMAN, FAHMIDA

ART UNIT PAPER NUMBER

2116

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/734,960

Applicant(s)

CHALLENGER ET AL.

Examiner

Fahmida Rahman

Art Unit

2116

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 5/3/2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>12/12/2003</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1-24 are pending.

### **Drawings**

2. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. Applicant discussed the possible problems associated with Fig 1 in Background Information and indicated the need to improve the security of Fig 1 by detecting modifications in legacy BIOS after booting of the system upon exiting of the sleep state. See MPEP § 608.02(g).

The drawings are objected to because Fig 1 shows reference numeral 20 to both platform and Add-On Cards.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the

Art Unit: 2116

remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-2, 4-7, 9-10, 12-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admission of Prior Art (AAPA), further in view of Balard et al (US Patent Application Publication 2004/0025036).

For claim 1, AAPA teaches the following limitations:

A method for detecting modifications to code placed in memory by the Power On Self Test (POST) Basic Input/Output System (BIOS) ([0016] of page 2) comprising the steps of:

- initiating said POST operation (lines 1-5 of [0013]);
- retrieving code from a flash memory (36 is within 42. 36 is retrieved from flash memory so that it can be measured);

Art Unit: 2116

- measuring said retrieved code to generate a first measurement (line 1 of [0014] of page 2);
- storing said first measurement in a secure area (line 13 of [0013] mentions that boot PCR 48 stores measurement. Boot PCR is secure);
- storing said retrieved code in a memory located in a non-secure area (lines 4-6 of [0014] of page 2 mention that BIOS code in 42 is moved to memory 33);

AAPA does not teach the following limitations:

- measuring said retrieved code stored in said memory located in said non-secure area after receiving an awakening event to generate a second measurement;
- and indicating said retrieved code stored in said memory was modified if said first measurement is not equal with said second measurement.

Balard et al teach the following limitations:

- measuring retrieved code (90, 236) stored in memory (14) located in non-secured area (14 is not secured, since firmware can be modified as mentioned in [0066] of page 5) after receiving an awakening event (204; [0081] of page 6, 54) to generate a second measurement (132)
- and indicating said retrieved code stored in said memory was modified ([0066] of page 5) if said first measurement (130) is not equal with said second measurement (132).

Art Unit: 2116

It would have been obvious for one ordinary skill in the art at the time the invention was made to combine the teachings of AAPA and Balard et al. One ordinary skill in the art would have been motivated to measure the retrieved code after receiving an awakening event to generate a second measurement to indicate if the retrieved code is modified, since that prevents alteration of firmware after initiation ([0099] of page 7 of Balard et al).

For claim 2, [0069] of page 5 of Balard et al mentions that 52 runs after reset and boot firmware executes in 96.

For claim 4, 64 of Balard et al comprises a reset to retrieve the proper code ([0063] of page 5).

For claim 5, AAPA mentions that the code is a "legacy BIOS code" ([0014] of page 2).

For claim 6, AAPA mentions that the code supports USB interface and power management ([0014] of page 2).

For claim 7, AAPA shows that the 48 is in TBB (Fig 1).

Claims 9-10, 12-15 are directed to the program product embodied in a machine readable medium corresponding to the method recited in claims 1-2, 4-7. For a

Art Unit: 2116

computer-implemented method, the associated code must be stored within a machine-readable medium. Thus, the cited references that teach 1-2, 4-7, also teach claims 9-10, 12-15.

For claim 17, AAPA teaches the following limitations:

A system, comprising:

- a memory (33);
- a processor (32) coupled to said memory;
- a first portion (36) of a flash memory (42) coupled to said processor, wherein said first portion of said flash memory comprises a Power On Self Test (POST) Basic Input/Output System (BIOS) code (36);
- and a Trusted Building Block (TBB) (40) coupled to said processor, wherein said TBB is configured to ensure integrity of said system ([0013], [0014], [0015] of page 1), wherein said TBB comprises:
  - a second portion (50) of said flash memory, wherein said second portion of said flash memory in said TBB comprises::
  - a boot block code (50), wherein said boot block code comprises code to reset said system; and code to be moved from said second portion of said flash memory to said memory by said POST BIOS code during a POST operation ([0014] of page 2);

- wherein said processor, responsive to said POST BIOS code, comprises:  
circuitry operable for retrieving said code from said second portion of said flash memory during said POST operation ([0013] and [0014] of page 1);
- circuitry operable for measuring said retrieved code to generate a first measurement ([0013] and [0014] of page 1);
- circuitry operable for storing said first measurement in a secure area;
- and circuitry operable for storing said retrieved code in said memory (processor 32 must have associated circuitry to perform the intended function);

AAPA does not teach the following limitations:

- measuring said retrieved code stored in said memory located in said non-secure area after receiving an awakening event to generate a second measurement;
- and indicating said retrieved code stored in said memory was modified if said first measurement is not equal with said second measurement.

Balard et al teach the following limitations:

- circuitry operable for measuring retrieved code (90, 236) stored in memory (14) located in non-secured area (14 is not secured, since firmware can be modified as mentioned in [0066] of page 5) after receiving an awakening event (204; [0081] of page 6, 54) to generate a second measurement (132)



Art Unit: 2116

- processor comprising circuitry operable for indicating said retrieved code stored in said memory was modified ([0066] of page 5) if said first measurement (130) is not equal with said second measurement (132).

It would have been obvious for one ordinary skill in the art at the time the invention was made to combine the teachings of AAPA and Balard et al. One ordinary skill in the art would have been motivated to measure the retrieved code after receiving an awakening event to generate a second measurement to indicate if the retrieved code is modified, since that prevents alteration of firmware after initiation ([0099] of page 7).

For claim 18, [0069] of page 5 of Balard et al mentions that 52 runs after reset and boot firmware executes in 96.

For claim 20, 64 of Balard et al comprises a reset to retrieve the proper code ([0063] of page 5).

For claim 21, AAPA mentions that the code is a "legacy BIOS code" ([0014] of page 2).

For claim 22, AAPA mentions that the code supports USB interface and power management ([0014] of page 2).

For claim 23, AAPA shows that the 48 is in TBB (Fig 1).

Art Unit: 2116

4. Claims 3, 8, 11, 16, 19, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admission of Prior Art (AAPA), further in view of Balard et al (US Patent Application Publication 2004/0025036), further in view of ordinary skill in the art.

For claims 3 11 and 19, Balard et al do not explicitly mention that the indication comprises error message. However, one ordinary skill in the art would have been motivated to have a system with error message, since that acts as an alert to the user.

For claims 8, 16 and 24, Ballard et al uses e-fuse array 24 and ROM 22 as the secured area, since these cannot be updated by anyone. However it would have been obvious for one ordinary skill in the art to modify them as lockable EPROM, since that would provide the flexibility to the authorized user to change the content, at the same time not accessible by the unauthorized user.

### **Conclusion**

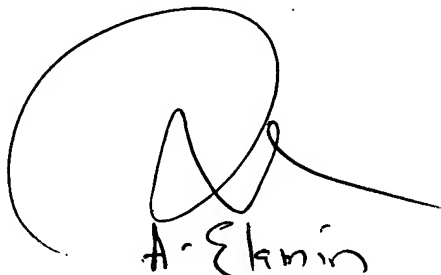
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fahmida Rahman whose telephone number is 571-272-8159. The examiner can normally be reached on Monday through Friday 8:30 - 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lynne Browne can be reached on 571-272-3670. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fahmida Rahman  
Examiner  
Art Unit 2116

4/17/06  
\*\*\*



A. Elmin  
Primary Examiner  
2116